Fatec Americana — Centro Paula Souza — Governo de São Paulo

Segurança da Informação

ESTUDO SOBRE INFECÇÃO DE VÍRUS DE COMPUTADOR DO TIPO RANSOMWARE

Lucas Fernando Messias

Americana

2015

Segurança da Informação

ESTUDO SOBRE INFECÇÃO DE VÍRUS DE COMPUTADOR DO TIPO RANSOMWARE

Lucas Fernando Messias

Monografia de conclusão de curso apresentado à Banca Examinadora do Curso de Segurança da Informação – da Faculdade de Tecnologia de Americana, como requisito para obtenção de título de tecnólogo em Segurança da Informação.

Orientação: Prof. Ms. Henri Alves de Godoy

Americana

2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Messias, Lucas Fernando

M548 Estudo sobre Infecção de vírus de computador do tipo Ransomware. / Lucas Fernando Messias. – Americana: 2015.

f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Me. Henri Alves de Godoy

1. Segurança em sistemas de informação I. Godoy, Henri Alves de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Lucas Fernando Messias

ESTUDO SOBRE INFECÇÃO DE VÍRUS DE COMPUTADOR DO TIPO RANSOMWARE

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação.

Americana, 10 de Dezembro de 2015.

Banca Examinadora:

Henri Alves de Godoy (Presidente)
Mestre
Fatec Americana

Juliane Borsato Beckedorff Pinto (Membro)
Graduada
Fatec Americana

Valderes Aparecida Rinaldi (Membro)
Especialista
Fatec Americana

RESUMO

Esta monografia teve por objetivo demonstrar a infecção do vírus de computador, do tipo Ransomware. Para fins de realizações de testes, criou-se um ambiente com máquina virtual, onde pode-se realizar testes com uma versão de vírus da família Ransomware. Obter um diagnostico e compreender o processo de infecção e posteriormente a encriptação dos arquivos da máquina infectada. Tendo como base pesquisas bibliográficas em livros e sites na Internet esta monografia consiste em propor uma avaliação da infecção vírus da família Ransomware, além da criptografia RSA utilizada por este para sequestrar os dados de sua vítima. Também entender o que é Bitcoin e por que estes pedidos de resgates são feitos em Bitcoin. Com o objetivo de precaver futuras infecções deste tipo de vírus, a utilização algumas ferramentas e boas práticas podem fazer a diferença no dia a dia, mas não deixa de ser imprescindível que se tenha a prática de realizações de backups, que além de salvos localmente, devem ser salvos em outros tipos de mídias, como HD externo, servidores em nuvem, caso o vírus venha corromper arquivos de backup e venha ocasionar total perda.

Palavras chaves: Ransomware; RSA; Vírus de computador; Bitcoin.

ABSTRACT

This monography intends to demonstrate the viruses computer infection, of Ransomware type. For testing achievement purposes, a virtual machine environment was created, where it was possible to perform tests with a version of Ransomware family virus. It generate a diagnosis that helped to understand the infection process and also enable the files encryption from the infected machine. Based on bibliographic research in books and websites this monography consists of proposing an assessment of infection from any viruses of Ransomware family, and also comprehends the RSA encryption used for kidnap data from its victim. Also it intends to explain what is Bitcoin and why these redemptions requests are made using it. In order to avoid future infections of this virus type, the use of some tools and good practices can make a difference in daily activities, but it`s essential to have the backup practices, which in addition to store locally, must be saved in other types of media, such as external HD, cloud servers, because if the virus come to corrupt backup files it can cause total loss

Keyword: Ransomware; RSA; Viruses computer; Bitcoin.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Na era da tecnologia, as organizações passam a ter a informação como um dos seus principais patrimônios. Sendo um dos principais ativos, a informação necessita ser protegida a qualquer custo de qualquer eventualidade. A perda das informações de uma organização acarreta um grande prejuízo para a mesma.

Quando começamos a trabalhar em organizações, precisamos nos lembrar de que a informação é um bem, tem valor para a empresa e deve ser protegida. A informação deve ser cuidada por meio de políticas e regras. Com isso queremos dizer que a informação é um ativo de valor. É um recurso crítico para a realização do negócio e a execução da missão da organização (FONTES, 2006).

Segundo Sêmola (2003), Segurança da informação entende-se em adotar controles físicos, tecnológicos e humanos personalizados, que viabilizem a redução e administração de riscos, levando a empresa a atingir o nível de segurança adequado ao seu negócio. Podemos também considerá-la como uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade, e ponderá-la como prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação.

Este estudo sobre a ocorrência de infecção de vírus de computador, conhecido como Ransomware, que usa a criptografia assimétrica para sequestrar as informações de suas vítimas, objetiva demonstrar os impactos que podem ocorrer com os dados que venham a ser corrompidos por este tipo de ataque. Para atenuar este tipo de ameaça, um estudo sobre o mecanismo do vírus será realizado, pois é quase impossível descriptografar os arquivos mantidos reféns. Com essas informações, é possível melhorar brechas de segurança que uma infraestrutura de rede possa ter contra este tipo de ataque, mantendo a integridade dos dados.

1.1 Problematização

Em uma empresa desenvolvedora de software para escritórios contábeis de pequeno e médio porte notou-se que o ataque de um tipo de vírus específico em alguns de seus clientes está causando intermitência no software disponibilizado pela empresa em seus adquirentes. Percebeu-se, também, que a infecção deste vírus é devastadora pelo fato de criptografar arquivos, com extensões *.doc, *.xls, *.jpg, e outros, utilizando uma cifra de Rivest, Shamir e Adleman (RSA) 1024 bits ou 2048 bits.

Este problema está estreitamente relacionado à Segurança da Informação, pois para as empresas ou usuários de redes domésticas que tem os seus dados criptografados, devido à infecção deste vírus, o impasse está na **integridade** das informações. Uma infecção por vírus deste tipo pode ocasionar que tipo de perda?

No mundo empresarial perdas relacionadas aos serviços prestados, dados sigilosos corrompidos que comprometem a continuidade do negócio. Para os usuários domésticos arquivos com informações pessoais corrompidos. Fica a pergunta: como abordar este problema e mitigar o impacto que pode ter a infecção deste vírus de computador?

Assimilando o conteúdo de estudo com as informações obtidas através de pesquisa é possível compreende-se do impacto causado por este vírus com o seu avanço tecnológico na criptografia utilizada e com essas informações melhorar brechas de segurança em uma infraestrutura de rede de computadores venha a ter.

2 Objetivo Geral

O objetivo geral deste trabalho é demonstrar os impactos que podem ocorrer com o ativo informação após infecção de vírus de computador, do tipo

Ransomware, que utiliza criptografia assimétrica RSA 1024 bits ou 2048 bits para criptografar vários tipos de extensões de arquivos da máquina ou rede infectada, comprometendo os dados e mantendo-os refém, pois solicita resgate em moeda digital da vítima para que seja liberado um software, que teria a chave privada e assim descriptografar os arquivos quais foram criptografados.

2.1 Objetivos específicos

Com o intuito de medir os impactos causados pela infecção do vírus, do tipo Ransomware*,* ao ativo informação, faz-se necessário:

- Entender a criptografia utilizada, visando à proposta de solução para o problema proposto;

- Analisar o grau potencial desta criptografia;

- Avaliar a tecnologia empregada no vírus, conhecendo suas ações e feitos;

- Analisar os danos causados por ele para a organização, objetivando redução de prejuízos;

- Propor melhorias de segurança na infraestrutura de rede de computadores, tentando evitar que o vírus se alastre pela rede para não corromper dados interno e deteriorar todo um sistema com informações importantes para o negócio ou pessoal, o que servirá como base para outras empresas.

3 Criptografia e conceito

O termo **criptografia** surgiu da fusão das palavras gregas "kryptós" e "gráphein" que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que

somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la.

A criptografia pode ser entendida como um conjunto de métodos e técnicas para cifrar ou codificar informações legíveis por meio de um algoritmo, convertendo um texto original em um texto ilegível, sendo possível mediante o processo inverso recuperar as informações originais (SIMON, 1999).

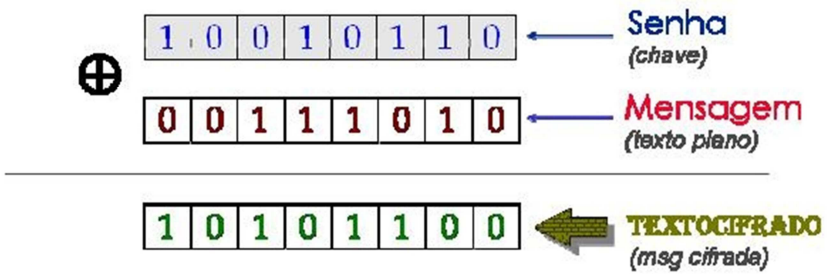
A criptografia é um mecanismo de segurança que permite a implementação de diversos serviços (autenticação, não repúdio, integridade, confidencialidade e âncora temporal).

Podem-se criptografar informações basicamente por meio de código ou de cifras. Os códigos protegem as informações trocando partes destas por códigos predefinidos. Todas as pessoas autorizadas a ter acesso a uma determinada informação devem conhecer os códigos utilizados.

As cifras são técnicas nas quais a informação é cifrada por meio da transposição e/ou substituição das letras da mensagem original. Assim, as pessoas autorizadas podem ter acesso às informações originais conhecendo o processo de cifragem. As cifras incluem o conceito de chaves.

A Figura 1 ilustra um exemplo de como pode ser aplicada a chave para cifrar um texto. Aplica-se a operação matemática de “ou exclusivo” entre a chave e o texto plano. O resultado é o texto cifrado. Para decodificar o texto cifrado, basta realizar o procedimento inverso, aplicando a operação de “ou exclusivo” entre o texto cifrado e a chave.

Figura 1 – Cifra “ou exclusivo”



Fonte: PKI – Public Key Infrastructure[1]

1 – Disponível em: < http://www.gta.ufrj.br/grad/07_2/delio/Criptografia.html >. Acesso em: 5 set. 2015

3.1 Criptografia simétrica

Segundo Nunes (2007), para proteger uma informação, garantindo a privacidade ou confidencialidade, é necessário um algoritmo de criptografia capaz de transformar a mensagem original em uma mensagem cifrada, ou seja, não compreensível por uma terceira entidade. O método ou algoritmo para cifrar e decifrar é chamado de cifra.

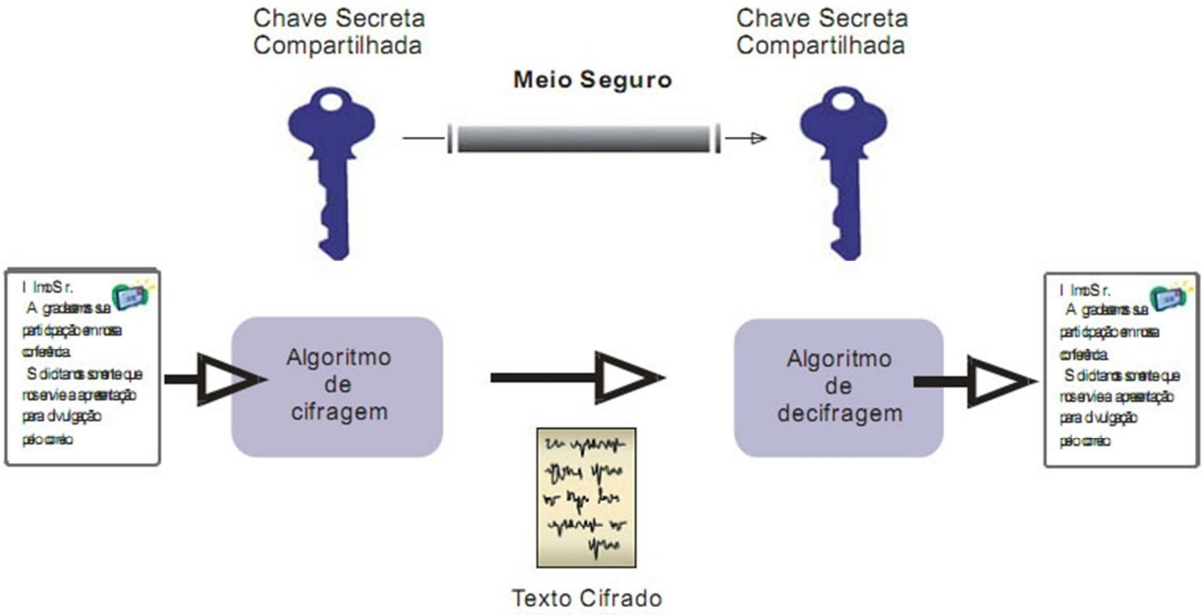
Alguns métodos criptográficos baseiam-se no segredo dos algoritmos. Estes algoritmos têm apenas interesse histórico e não são adequados para as necessidades do mundo atual, pois descobrindo o algoritmo pode-se abrir qualquer texto cifrado.

Todos os algoritmos modernos usam uma chave para controlar o ato de cifrar e decifrar. Isto é, uma mensagem só pode ser decifrada se a chave for à mesma que a utilizada para cifrar, ao contrário da criptografia antiga, onde o segredo era o algoritmo.

Os algoritmos criptográficos atuais são projetados para serem executados por computadores ou por dispositivos especializados de hardware. Na maioria das aplicações, a criptografia é realizada através de software de computador. De modo geral, os algoritmos simétricos são executados muito mais rapidamente que os assimétricos.

A Figura 2 demonstra o processo de funcionamento da criptografia simétrica.

Figura 2 – Mecanismo de criptografia simétrica



Fonte: PKI – Public Key Infrastructure[1]

3.1.2 Criptografia assimétrica

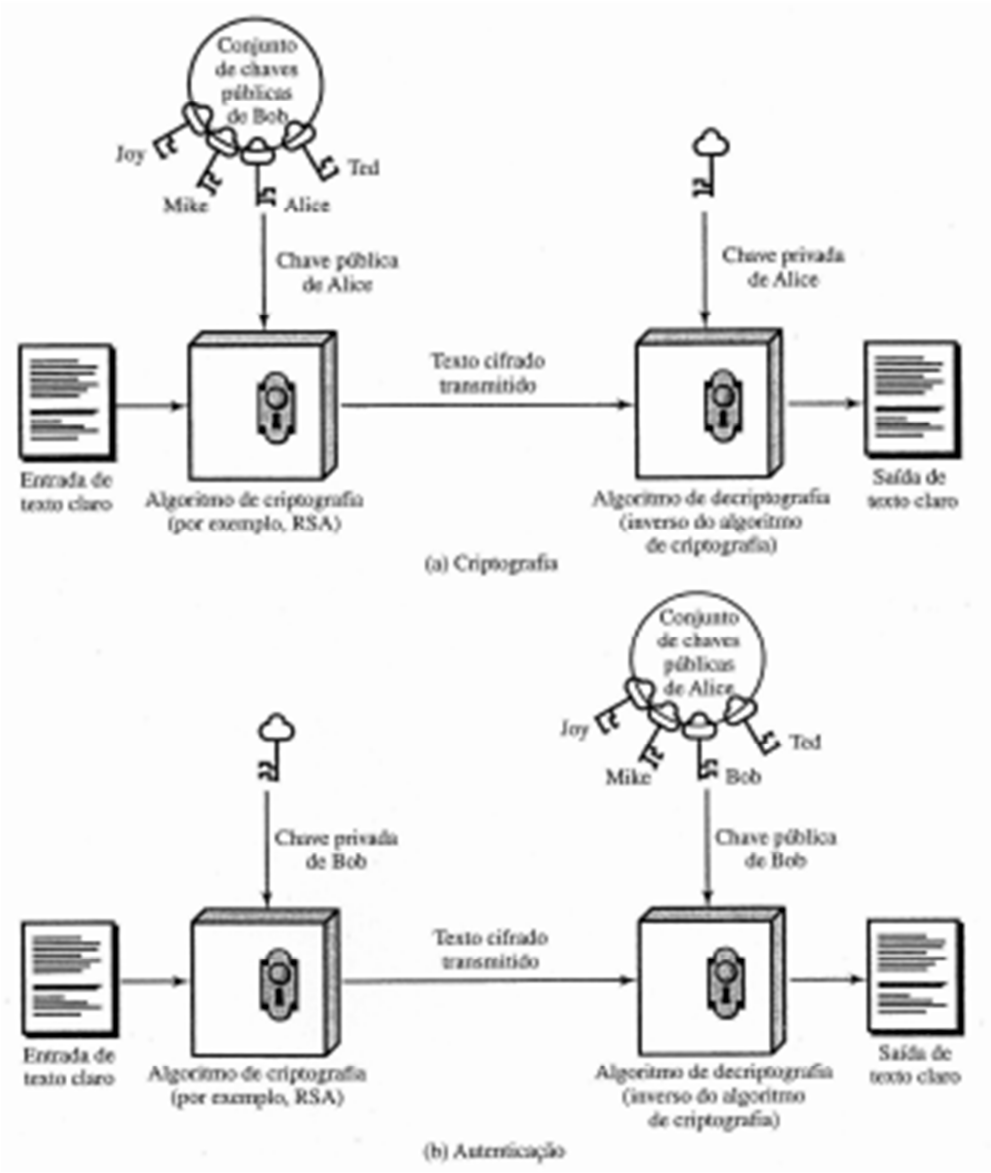
Em 1976, Diffie e Hellman mudaram os rumos da criptografia com a criptografia assimétrica, também chamada de criptografia de chave pública, eles propuseram um sistema para cifrar e decifrar uma mensagem com duas chaves distintas, sendo a pública (chave pública) que pode ser divulgada e a outra mantida em segredo (chave privada).

Funcionando da seguinte forma: se cifrar a mensagem com a chave privada ela somente será decifrada pela chave pública e vice-versa (NUNES, 2007).

1 – Disponível em: < http://www.gta.ufrj.br/grad/07_2/delio/Criptografiasimtrica.html >. Acesso em: 5 set. 2015

Segundo Stallings (2007), a criptografia assimétrica transforma o texto claro em texto cifrado usando uma de duas chaves e um algoritmo de criptografia. Usando a outra chave associada e um algoritmo de decriptografia, o texto claro é recuperado a partir do texto cifrado. A criptografia assimétrica pode ser usada para confidencialidade, autenticação ou ambos. A Figura 3 ilustra o processo de funcionamento da criptografia assimétrica.

Figura 3 – Mecanismos de criptografia assimétrica



Fonte: Stallings. (2007, p. 166)

3.1.3 Criptografia RSA

Em 1997, Rivest, Shamir e Adleman desenvolveram um algoritmo assimétrico denominado RSA, em referência aos sobrenomes dos autores. O algoritmo RSA é a base atualmente, da maioria das aplicações que utilizam criptografia assimétrica (NUNES, 2007). O tamanho da chave varia entre 512 bits a 2048 bits.

No caso esse estudo, o vírus Ransomware utiliza um tamanho de chave que varia entre 1024 bits a 2048 bits, em alguns casos além da criptografia RSA utilizados, o vírus utiliza outra variância de criptografia unida com a criptografia RSA, que é a criptografia simétrica AES. Elementos básicos de um esquema de criptografia de chave pública são:

(A) produz uma mensagem em texto claro, X=[X1, X2, X3, ..., Xm], onde "m" são elementos de X que são letras de algum alfabeto finito.

(A) deseja enviar uma mensagem destinada a (B) criptografada, para isso, (B) gera o par de chaves, que serão uma chave pública (PUb) e, uma chave privada (PRb), está somente será conhecida por (B).

Com a mensagem X e a chave pública (PUb) como entrada, (A) forma o texto cifrado Y=[Y1, Y2, Y3, ..., Yn]

Y = E(PUb, x), onde:

Y = Texto cifrado
E = Algoritmo
PUb, x = chave pública + texto claro

O receptor a quem se destina a mensagem é capaz de inverter o texto, de posse da chave privada (PRb).

X = D(PRb, Y), onde:

X = Texto claro

D = Algoritmo

PRb, Y = Chave privada + texto cifrado

Com a criptografia de chave pública poderá se obter segurança e autenticidade, onde podemos classificar o seu uso em três categorias:

- Encriptação - decriptação: o remetente encripta a mensagem com a chave pública do beneficiário.
- Assinatura digital: o remetente "assina" a mensagem com a sua chave privada. Assinatura é atingida de um algoritmo criptográfico aplicado para a mensagem ou para um pequeno bloco de informação.
- Troca de chaves: cooperação para troca de chaves, muitas aproximações são possíveis, envolvendo chave privada de um para o outro participante.

O RSA é uma cifra de bloco em que, o texto simples e texto encriptado são inteiros entre (*0 e n -1 para algum n*). O esquema de desenvolvimento por Rivest, Shamir e Adleman faz o uso de expressões com exponenciais, o texto simples é encriptado em blocos, com cada bloco contendo um valor binário menor que *(n)*. O tamanho do bloco deve ser menor ou igual para log²(n). Na prática o tamanho é 2^k bits, onde 2^k < n <= 2^{k+1} .

O processo de encriptação e decriptação são feitos da seguinte forma, para algum texto simples bloco M é encriptado bloco C.

$C = M^e$ *mod (n)*, para obter o texto/bloco criptografado.

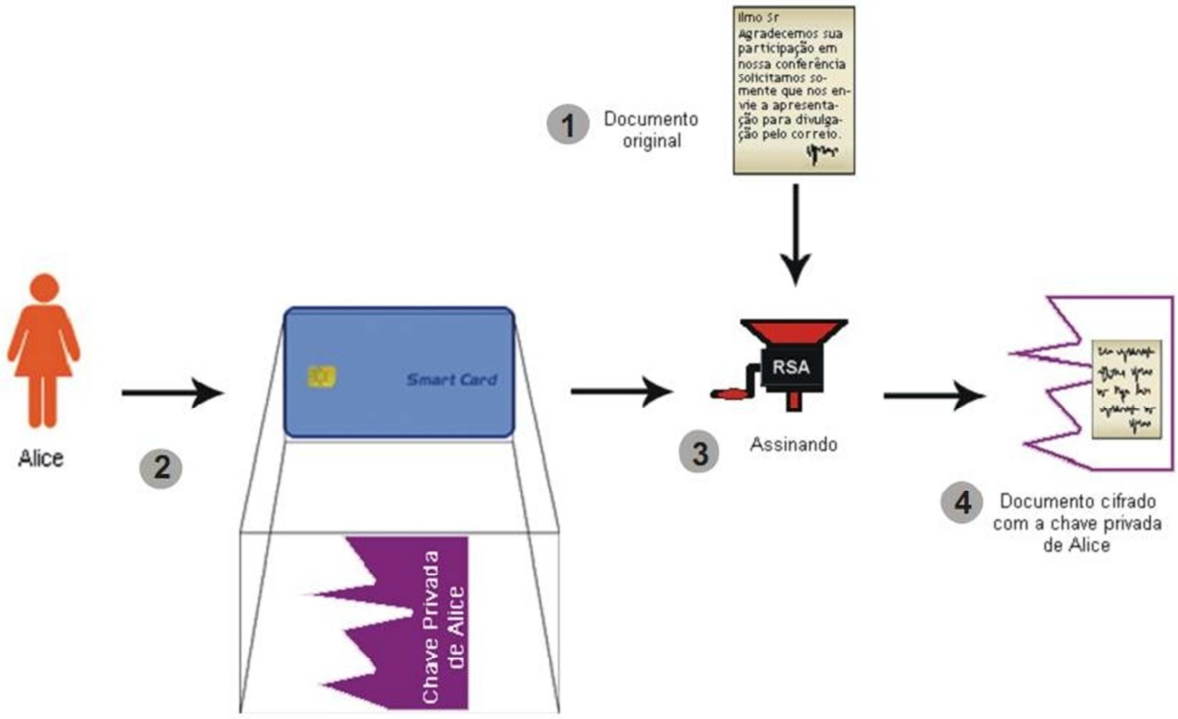
$M = C^d$ *mod (n)* = $(M^e)^d$ *mod n* = M^{ed} *mod n*, para obter o texto/bloco claro.

Ambos, remetente e receptor devem conhecer o valor de *n,* o remetente deve saber o valor de (*e*), e somente o receptor deve saber o valor de (*d*). Assim este algoritmo de encriptação de chave pública, com a chave pública *KU={e,n},* e a privada *KR={d,n},* para este algoritmo ser satisfatório para encriptação de chave pública, os seguintes requisitos devem ser conhecidos:

- É possível encontrar os valores de *(e, d, n)* de tal modo que M^{ed} *mod n* para todo *n* < *n.*
- É relativamente fácil calcular M^e *e* C^d para todos os valores de *M* < *n.*
- É inviável determinar *(d)* dado *(e)* e *(n).*

Um texto claro pode ser cifrado a partir da chave privada, onde só será decifrado com a chave pública e vice-e-versa. Garantindo integridade e autenticidade. A Figura 4 demonstra o funcionamento de uma cifra com chave privada.

Figura 4 – Cifrar com chave privada:



Fonte: PKI – Public Key Infrastructure[1]

1. Disponível em: <http://www.gta.ufrj.br/grad/07_2/delio/Criptografiaassimtrica.html >. Acesso em: 5 set. 2015.

A função RSA para cifrar, utilizando chave privada é a seguinte:

$C = M^d$ *(mod n),* onde:

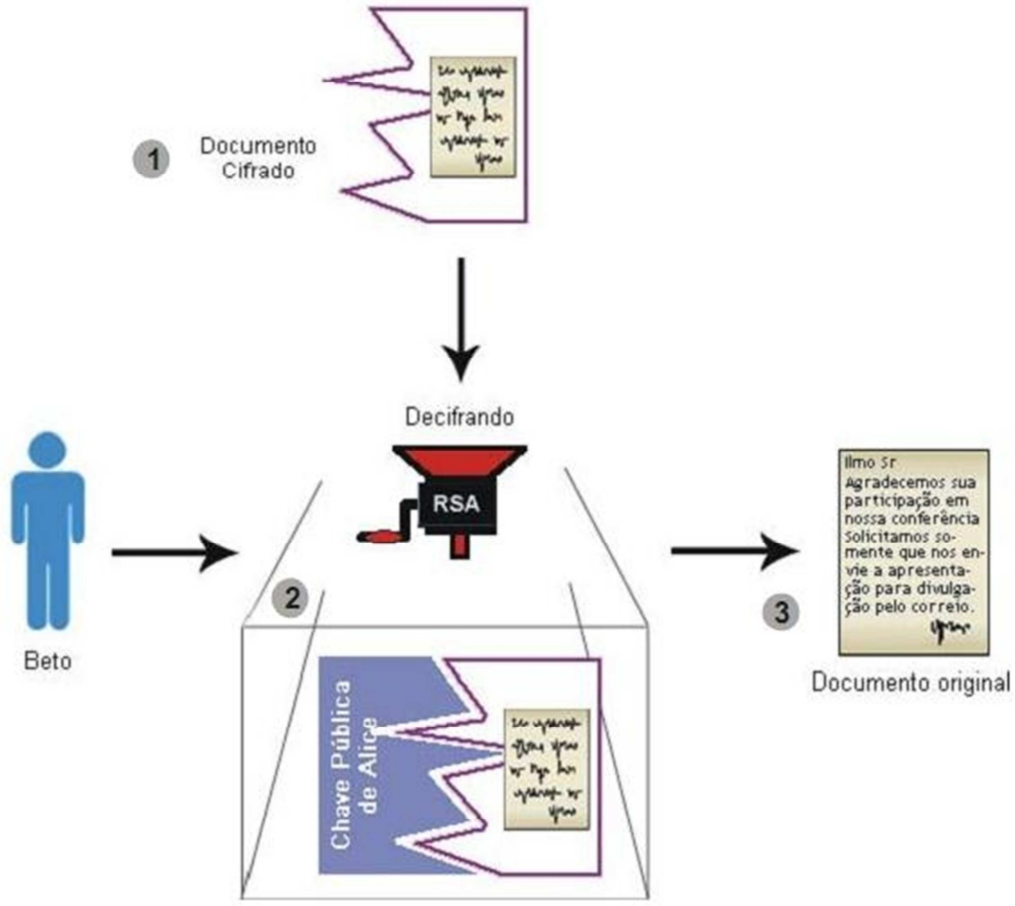
C = texto cifrado

M = texto plano (texto claro)

"d" e "*n"* = chave privada *KR={d, n}*

Quando se deseja decifrar um documento que foi cifrado com a chave privada utiliza-se a chave pública. A Figura 5 demonstra como decifrar com chave pública.

Figura 5 – Decifrar com chave pública:



Fonte: Fonte: PKI – Public Key Infrastructure[1]

1. Disponível em: < http://www.gta.ufrj.br/grad/07_2/delio/Criptografiaassimtrica.html >. Acesso em: 5 set. 2015.

A função RSA para decifrar, utilizando a chave pública é a seguinte:

$M = C^e$ *(mod n),* onde:

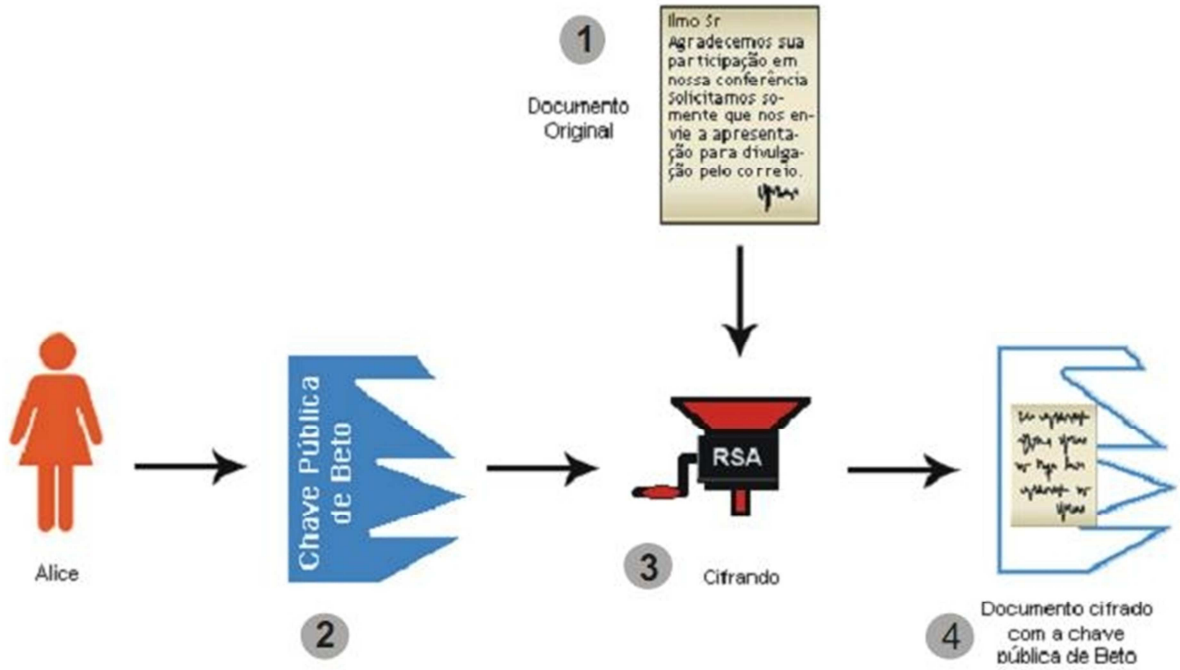
M = texto plano (texto claro)

C = texto cifrado

"e" e *"n"* = chave pública *KU={e, n}*

A Figura 6 demonstra o funcionamento de uma cifra com chave pública.

Figura 6 - Cifrar com chave pública:



Fonte: PKI – Public key infrastructure[1]

A função RSA para cifrar, utilizando a chave pública, é a seguinte:

$C = M^e$ *(mod n),* onde:

C = texto cifrado

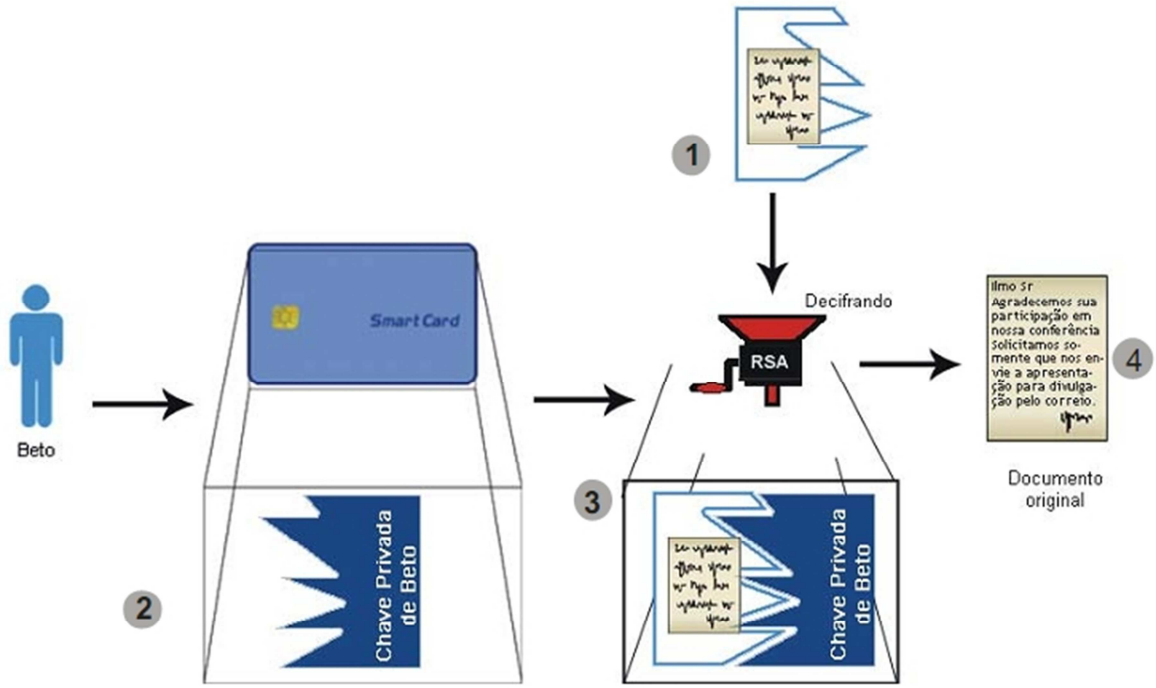
1. Disponível em: < http://www.gta.ufrj.br/grad/07_2/delio/Criptografiaassimtrica.html >. Acesso em: 5 set. 2015.

M = texto plano (texto claro)

“*e*” e “*n*” = chave pública *KU={e, n}* do destinatário.

Quando se deseja decifrar um documento que foi cifrado com a chave pública utiliza-se a chave privada. A Figura 7 demonstra como decifrar com chave privada.

Figura 7 – Decifrar com chave privada:



Fonte: PKI – Public key infrastructure[1]

A função RSA para decifrar, utilizando a chave privada é a seguinte:

$M = C^d$ *(mod n),* onde:

M = texto plano (texto claro)

C = texto cifrado

“*d*” e “*n*” = chave privada *KU={d, n}.*

1. Disponível em: < http://www.gta.ufrj.br/grad/07_2/delio/Criptografiaassimtrica.html >. Acesso em: 5 set. 2015.

4 Bitcoin

Bitcoin é uma moeda digital que surgiu na Internet, um sistema descentralizado, ou seja, não existe um grande servidor responsável pelo gerenciamento dela. Toda a rede de Bitcoins é *Peer to Peer (P2P)*[1] e isso garante que o sistema seja autorregulado.

Mantém o anonimato dos participantes e todas as transações são checadas para evitar cobrança dupla ou fraudes, além disso essas transações ficam disponíveis para checagem pública.

A falta de regulamentação também faz com que essa criptomoeda seja completamente livre de influências políticas ou fronteiras. Se ela está na Internet, está em todo mundo ao mesmo tempo. Não há uma autoridade central, governos ou bancos regulando ou intermediando negociações com Bitcoins.

4.1 Como são geradas as Bitcoins

Para entender esse processo é preciso compreender como a rede de Bitcoin funciona. Ela é formado por blocos encadeados uns nos outros. São esses blocos que carregam todas as informações, incluindo todas as transações já realizadas e todas as informações referentes ao processo. São mais ou menos como ouro, ou um metal precioso, elas têm que ser “garimpadas” nas Internet através de usuários de uma aplicação gratuita que libera Bitcoins em troca de um

1. P2P (ponto a ponto) é uma rede de computadores que compartilham arquivos pela Internet. Não há um servidor geral que os armazene e sim usuários que ao mesmo tempo que fazem o download, os disponibilizam para que outros busquem arquivos nas suas máquinas.

esforço computacional na resolução de problemas matemáticos complexos, que ajuda a verificar e divulgar todas as transações.

A rede possui um banco de dados que se expande em blocos, que são gerados mais ou menos a cada dez minutos e que contêm todas as transações realizadas, mantendo privacidade dos usuários, as trocas ficam abertas e podem ser checadas, uma medida de segurança para evitar que uma Bitcoin seja gasta duas vezes. A quantidade de fundos disponibilizada é ajustada em uma crescente previsível e controlada, apenas 21 milhões de Bitcoins serão criadas, com uma escala pré-definida sobre a liberação delas até 2040 (GIZMODO BRASIL, s.d).

4.1.2 A genealogia entre o Bitcoin e os hackers

A falta de uma autoridade central e a desregulação também atraiu criminosos e negócios ilegais para o Bitcoin, criando uma economia do anonimato. O pseudônimo[1] do Bitcoin é diferente das contas bancárias tradicionais, pois o titular e o número da conta não se encontram em nenhum banco de dados central. Cada usuário possuiu uma carteira digital que cria um número arbitrário de par de chaves pública e privada. As chaves privadas da carteira Bitcoin são senhas privadas usadas para autorizar pagamentos, exclusivamente pelo dono da moeda.

Os endereços são gerados pela carteira por um processo criptográfico arbitrário. Se um usuário quiser navegar de forma anônima na rede, é essencial que o usuário tome algumas medidas preventivas para esconder o seu endereço de IP de forma a obter privacidade máxima enquanto navega na Internet e não torna pública sua identidade real e seus endereços Bitcoin na Internet.

Por este motivo hackers tem a preferência pela moeda digital Bitcoin e, abrem portas para uma infinidade de atividades como a contratação de assassinos de aluguel, contrabando, compra de armamento e drogas.

1. Pseudônimo é nome adotado pelo autor ou responsável por uma obra (literária ou de qualquer outra natureza), que não use o seu nome civil verdadeiro ou o seu nome consuetudinário.

5 Vírus de computador

De acordo com Fontes (2006), vírus são programas que penetram no computador que utilizamos sem a nossa autorização e executam ações que não solicitamos. Normalmente, essas ações prejudicam o equipamento ou seu desempenho.

Muitos vírus abrem “portas dos fundos[1]”, criando uma forma de alguém acessar remotamente e assumir o controle do seu computador. Essa “porta dos fundos” pode habilitar atividades que variam entre abrir e fechar a unidade de CD-ROM e roubar ou excluir arquivos. Há ainda a possibilidade de um computador infectado ser transformado em um servidor de correio eletrônico para enviar *spams,* aguardando instruções do criador do vírus para encaminhar mensagens de *spam* (FEINSTEIN, 2004).

5.1 Propagação de um vírus

Antes da Internet, os vírus de computador se propagavam lentamente, de pessoa por pessoa, através de um meio físico para se propagarem. Por exemplo, um disquete infectado, que passava de pessoa por pessoa, aquelas máquinas qual o disquete era inserido o computador acaba sendo infectado pelo vírus, obviamente que a propagação se manifestava lentamente e normalmente, o impacto geral e a propagação de qualquer vírus eram limitados.

Atualmente como praticamente todos os computadores são conectados a Internet, os vírus se propagam com uma velocidade e ferocidade antes

1. Portas dos fundos, é um recurso utilizado por diversos *malwares* para garantir acesso remoto ao sistema ou à rede infectada, explorando falhas críticas não documentas existentes em programas instalados, *softwares* desatualizados e do *firewall* para abrir portas no roteador.

inimaginável. Uma vez que um vírus infecte um computador, pode pesquisar na Internet à procura de servidores Web com vulnerabilidades de seguranças e instalar-se naqueles servidores (FEINSTEIN, 2004).

De acordo com Rufino (2002), a forma mais comum de se propagar um vírus é por meio de mensagem eletrônica, mas apesar do e-mail ser a forma de propagação mais popular, certamente não é a única, e protocolos como FTP, POP3, e mesmo arquivos baixados via HTTP podem conter vírus.

5.1.2 Vírus Ransomware

Ransomware é um tipo de *malware*[1] que sequestra ou limita o acesso aos computadores e arquivos, onde que para recupera-los novamente, força suas vitimas pagarem um resgate relativamente alto para libera-los. Os preços variam de acordo com a versão do vírus Ransomware, mas pode variar entre $USD 24 até $USD 600, ou então o mesmo equivalente em Bitcoins. O primeiro caso de infecção deste tipo de vírus, ocorreu entre o ano de 2005 a 2006 na Rússia, uma variante do Ransomware, identificada como “TROJ_CRYZIP.A” que compactava os arquivos, deixando somente uma senha de proteção de acesso aos mesmos, também fazia a criação de um bloco de notas, solicitando o resgate, em forma de liberação dos arquivos, em troca de $300 dólares. De acordo com Castro, coordenador de Awareness & Research da Eset na América Latina, (EXAME, 2014):

> Esses vírus inicialmente bloqueavam apenas o acesso ao computador, usando uma espécie de tela de login “falsa”. Você não podia usar o PC, e precisava pagar certo valor para obter o acesso de volta. Mas naquele caso,

1. *Malware,* é um software destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roube de informações (confidenciais ou não).

> o usuário podia tirar o HD e conectá-lo em outro lugar para acessar os dados.
>
> Foi essa possibilidade que, de certa forma, fez os criminosos melhorassem a ideia por trás do Ransomware. O que eles querem hoje é que a informação seja criptografada. Você acessa o computador, seu sistema operacional, mas eles podem pegar uma unidade inteira de HD e bloqueá-la. E para poder abri-la novamente, é preciso usar uma chave, pela qual você precisar pagar um determinado valor dependendo do vírus.

5.1.3 Método de infecção

O Ransomware tem variedade de formas de infectar uma máquina, como uma falsa atualização para aplicativos como Adobe Reader, Flash Player ou o Java Runtime Environment. Esse tipo de atualização maliciosa pode ser oferecido em janelas *pop-up*[1] quando você visita sites inseguros ou quando um programa potencialmente indesejado é instalado no seu computador. O Ransomware também pode ser distribuído usando anexos de e-mail de *spam* e outros métodos típicos de entrega de ameaças (ENIGMAS SOFTWARE, s.d).

5.1.4 Encriptação dos arquivos

A encriptação dos arquivos inicia-se em uma ordem alfabética em todos os arquivos do usuário (word, excel, etc), incluindo pastas e unidades de disco rígido, além de pendrive's.

O processo de encriptação somente começará quando a máquina obtiver o acesso à Internet, caso contrário o vírus não produzirá nenhum resultado.

1. Pop-up, é uma janela que abre no navegador ao visitar uma página web. Utilizado pelos criadores do site para abrir alguma informação extra ou como meio de propaganda.

Somente quando a máquina obtém o acesso é que ele começa o processo com inúmeras chamadas a domínios em busca de *payloads*[1], e também para criar uma chave de criptografia. Para posteriormente começar o processo de encriptação dos arquivos do sistema, concluído o processo de encriptação, é realizado o pedido de resgate para decriptação dos arquivos infectados através de valores estipulados pelo criador do vírus, ou então, o equivalente em moeda eletrônica Bitcoin.

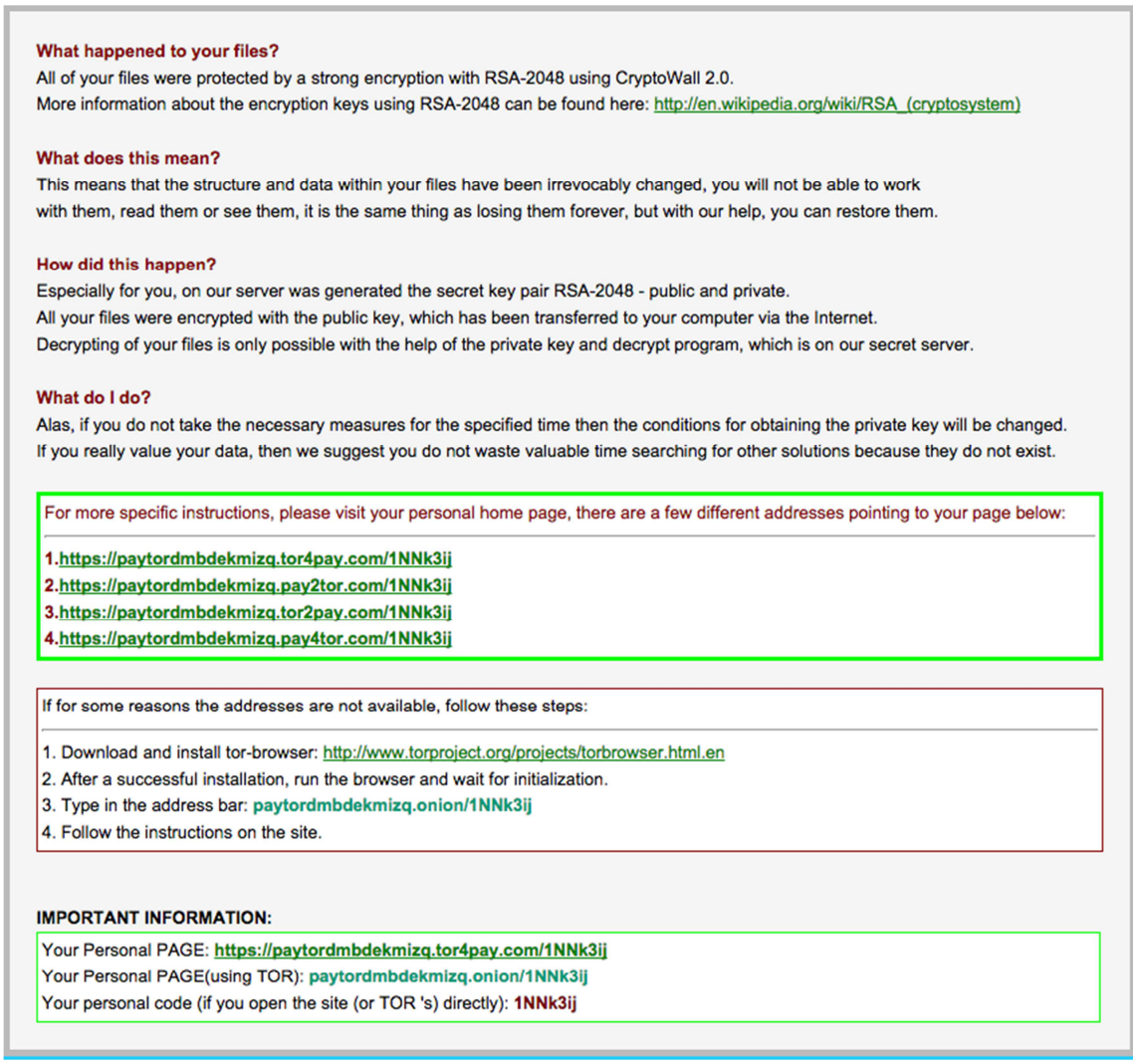
5.1.5 Ransomware Cryptowall 2.0

O primeiro caso de vírus Ransomware notificado no ano de 2015, foi pelo grupo de pesquisadores da Cisco, *Talos Security Intelligence and Research Group,* que divulgou em 6 de Janeiro de 2015, uma nova versão do vírus que ficou conhecida como *Cryptowall 2.0*, capaz de fazer a distinção entre arquitetura 32 bits e 64 bits e executar diferentes versões para cada tipo de sistema operacional, incluindo também a mais recente versão do Mac OS X(CISCO a, 2015).

O *Cryptowall 2.0* utiliza o navegador que permite navegar em anonimato para proteger sua privacidade (TOR), assim ofuscar o canal de comando e controle e, utiliza de múltiplos vetores de ataques, incluindo anexos de e-mail, arquivos PDF maliciosos, etc. Uma vez que o sistema era infectado, uma mensagem era apresentada para o usuário, similar a Figura 8:

1 – Disponível em: < http://blogs.cisco.com/security/talos/cryptowall-2> Acesso em Out. 2015.
2 – Hash MD5, é uma algoritmo de 128 bits não direcional desenvolvido pela RSA Data Security, Inc. Muito utilizado por softwares com protocolo P2P – peer to peer, na verificação de integridades dos arquivos e *logins.*

Figura 8 – Alerta com instruções pós-infecção cryptowall 2.0:



Fonte: Ransomware – Repositório digital da Cisco a[1]

O primeiro passo após ter a máquina infectada pelo vírus é a criação de um executável com o nome baseado em *hash MD5*[2] do computador. Este executável era copiado para um local especifico “%APPDATA%” da variável ambiente (“C:\Users\<Username>\AppData\Roaming”). Para manter-se sempre em execução, um valor de registro *auto-start* era adicionado:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

1 – Disponível em: < http://blogs.cisco.com/security/talos/cryptowall-2> Acesso em Out. 2015.
2 – Hash MD5, é uma algoritmo de 128 bits não direcional desenvolvido pela RSA Data Security, Inc. Muito utilizado por softwares com protocolo P2P – peer to peer, na verificação de integridades dos arquivos e *logins.*

O mesmo executável aleatório era copiado para a pasta *Inicializar do Menu Iniciar* . O último dever do falsificado processo “explorador” era desativar todas as proteções do sistema, executando os seguintes comandos de shell:

“vssadmin.exe Delete Shadows /All /Quiet

bcdedit.exe /set {default} recoveryenabled No

bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures”

Os seguintes serviços também são desabilitadas: Security Center, o Windows Defender, o Windows Update, Background Intelligent Transfer Service, ERSvc, o Windows Error Reporting Service

Finalmente o arquivo original é encerrado e excluído, o *Cryptowall 2.0* está agora injetado em um processo simulando ser um *Svchost*[1] da mesma forma como o falso “explorador” de processo foi criado inicialmente. A infecção continua agora no processo de falsificado *Svchos*[1]. (CISCO a, 2015).

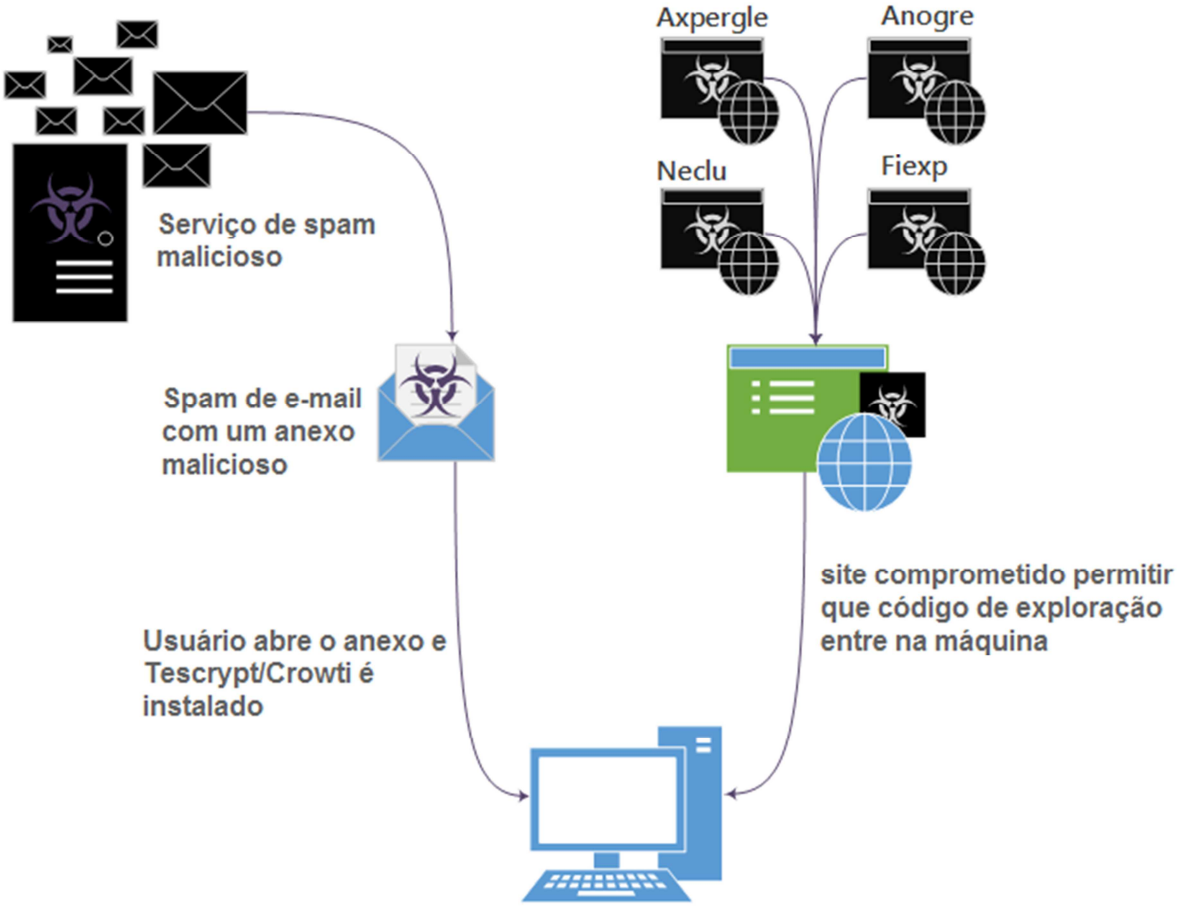
5.1.6 Ransomware Cryptowall 3.0

Segundo o Malware Protection Center da Microsoft (2015), dois tipos de vírus Ransomware, foram predominantes em 2015, o *Crowti* (também conhecido como *Cryptowall 3.0*) e o *Tescrypt* (também conhecido como *Telascrypt*), ambos são da família Ransomware que já infectaram meio milhão de computadores que executavam o software Microsoft Security até a primeira metade de 2015.

Ambos *Crowti* e *Tescrypt* são direcionados tanto para usuários domésticos quanto para indústrias corporativas, e ambos têm o processo de infecção semelhante, seus principais vetores de infecção são através de *spam* de e-mail e *exploit kits*[2]. Esta família de Ransomware criptografa os arquivos de computadores e direcionam as máquinas dos usuários para a *webpage* que solicita o pagamento utilizando o Bitcoin, conforme ilustrado na Figura 9:

1. Svchost, é um processo no computador que hospeda, ou contém, outros serviços individuais que o Windows usa para executar várias funções. Por exemplo, o Windows Defender usa um serviço que é hospeado por um processo svchost.exe.

Figura 9 – Processo de infecção do vírus *cryptwall 3.0*:



Fonte: Autoria própria adaptado de Ransomware – Microsoft, Malware Protection Center[1]

Depois que a máquina é infecta pelo *Cryptowall* 3.0, ele injeta código em processos do sistema, como *explorer.exe* ou *svchost.exe.* Uma cópia de nome aleatório do próprio vírus é instalada em qualquer um desses caminhos:

- c:\<random name>\<random name>.exe
- %APPDATA% \<random name>.exe
- <start menu> \programs\startup\<random name>.exe

Algumas modificações nos registros do Windows também são executadas toda vez que se inicia o computador:

HKU\Registry\User\<SID>\Software\Microsoft\Windows\CurrentVersion\Run Sets value: "<random name>". Com a informação: "c:\<random name>\<random name>.exe".

1. Disponível em: < https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx >. Acesso em: 20 out. 2015.

HKU\Registry\User\<SID>\Software\Microsoft\Windows\CurrentVersion\Run Sets value: "<random name>" Com informação: "c:\<random name>\<random name>.exe"

HKU\Registry\User\<SID>\Software\Microsoft\Windows\CurrentVersion\RunOnce Sets valor: "*<random name>" Com informação: "c:\<random name>\<random name>.exe"

Este *malware* pode criptografar os arquivos do computador usando uma chave pública. Os ficheiros podem ser descriptografados com a chave privada armazenada num servidor remoto. Abaixo podemos ver a Figura 10 com alguns exemplos de extensões de arquivos que este vírus pode criptografar.

Figura 10 – Extensões criptografadas pelo vírus *Cryptowall 3.0:*

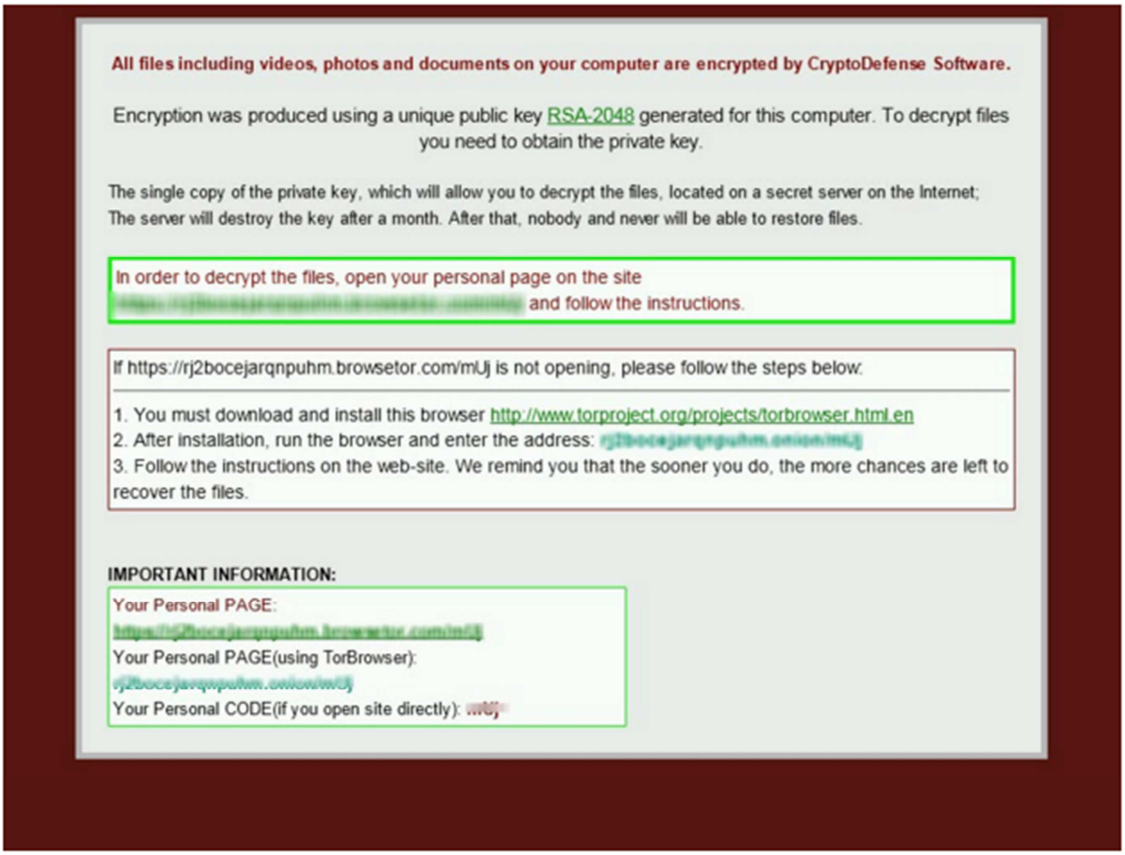
.asp	.gif	.pem
.ass	.h	.pl
.ava	.hpp	.png
.avi	.jpg	.ppt
.bay	.js	.ps
.bmp	.key	.py
.c	.lua	.RAW
.cer	.m	.rm
.cpp	.mp3	.rtf
.crt	.mpg	.sql
.cs	.msg	.swf
.db	.obj	.tex
.der	.odt	.txt
.doc	.PAS	.wb2
.DTD	.pdb	.wpd
.eps	.pdf	.xls

Fonte: Autoria própria adaptado de Microsoft, Malware Protection Center.

Em seguida, exibe uma tela de bloqueio semelhante à Figura 11, onde ilustra como você pode recuperar os arquivos usando um link pessoal que direciona para uma página web Tor[1] pedindo o pagamento usando Bitcoins como moeda.

1. Navegador TOR, é um software livre de código aberto para proteger o anonimato pessoal ao navegar na Internet e atividades online, protegendo contra censura e protegendo a privacidade pessoal.

Figura 11 – Instruções como recuperar arquivos pós-infecção *cryptowall* 3.0:

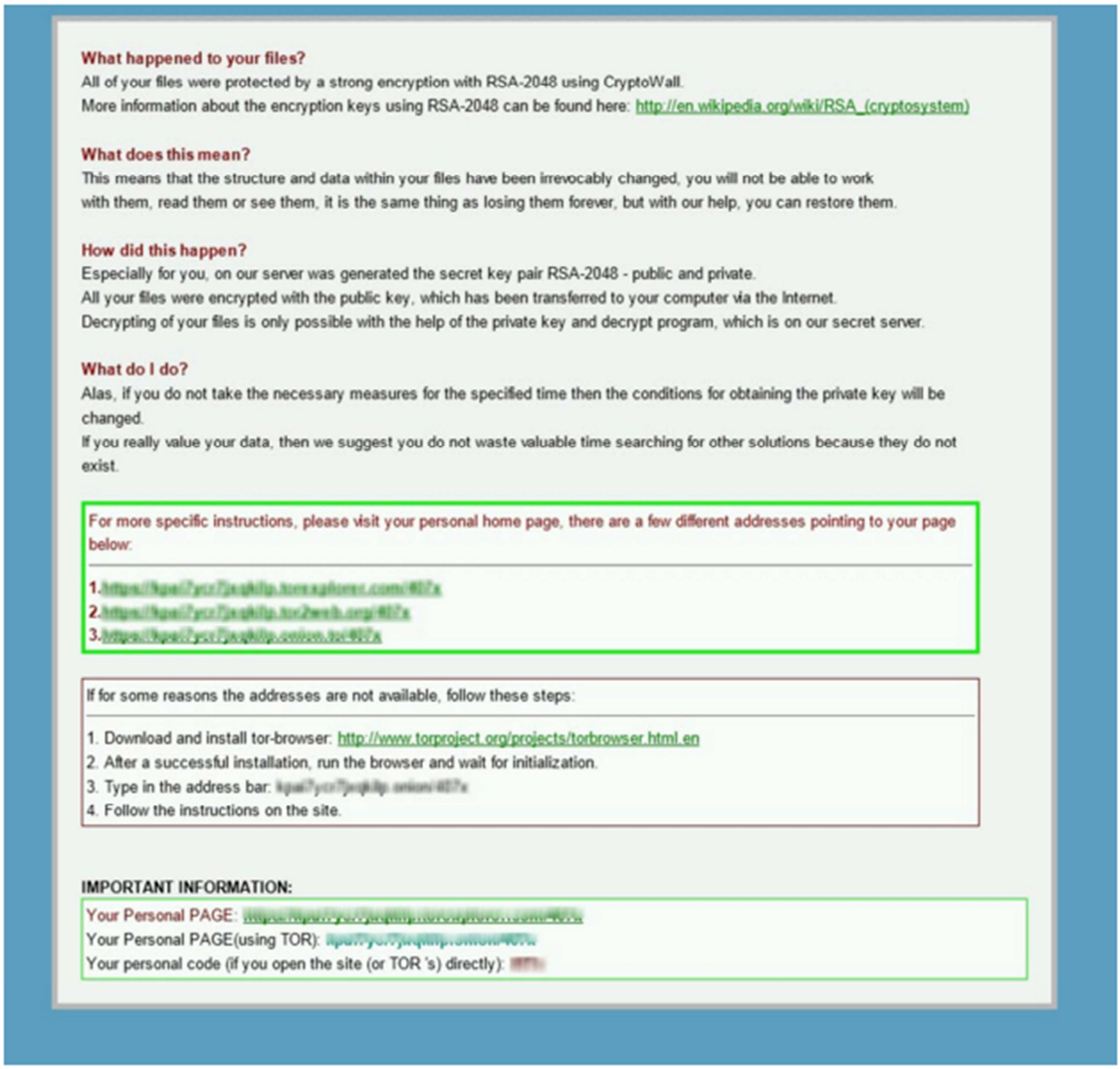


Fonte: Ransomware – Microsoft, Malware Protection Center[1]

A Figura 12 ilustra a mensagem que é apresentada quando se abre o arquivo de nota do vírus, que é criado em algum repositório que tenha sido infectado pelo vírus.

1. Disponível em: < https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Win32%2fCrowti#tab=2 > Acesso 20 out. 2015.

Figura 12 - Instruções como recuperar arquivos pós-infecção *cryptowall* 3.0:

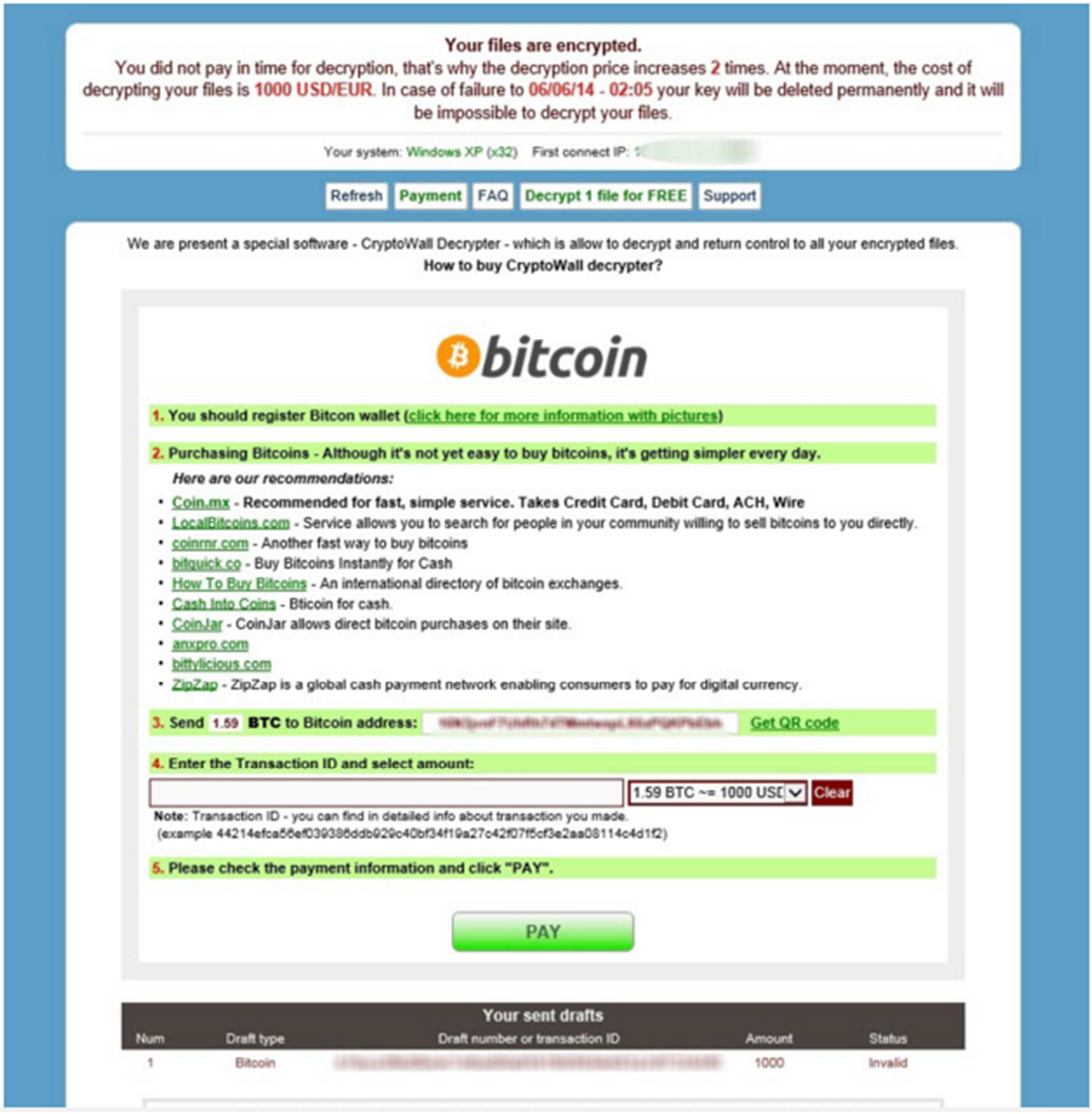


Fonte: Ransomware – Microsoft, Malware Protection Center[1]

Para recuperar os arquivos infectados muitas versões de vírus pedem o resgate em *Bitcoin*, é o que ilustra a Figura 13.

1. Disponível em: < https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Win32%2fCrowti#tab=2 > Acesso 20 out. 2015.

Figura 13 - Instruções como recuperar arquivos pós-infecção *cryptowall* 3.0:



Fonte: Ransomware – Microsoft, Malware Protection Center[1]

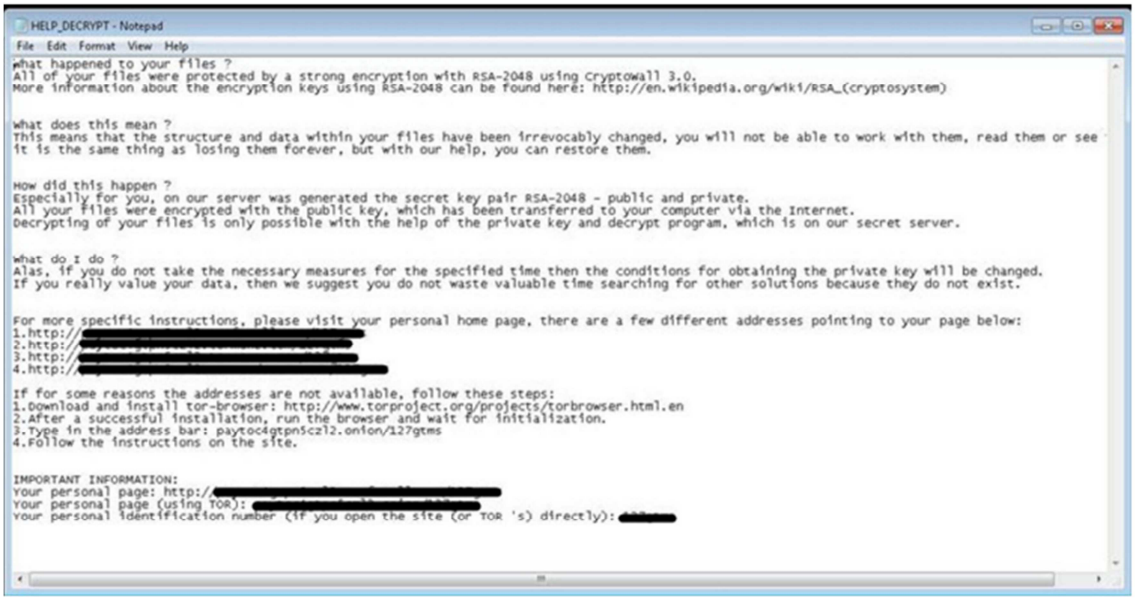
1. Disponível em: < https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Win32%2fCrowti#tab=2 > Acesso 20 out. 2015.

Cryptowall 3.0 também apaga arquivos de sombra Shadow Copy[1] do Windows para que não se tenha a possibilidade de restaurar os arquivos de um backup local. O mesmo utiliza os seguintes nomes de arquivo para seu apontamento de resgate, que contém instruções sobre como descriptografar os arquivos:

- DECRYPT_INSTRUCTION.HTML
- DECRYPT_INSTRUCTION.TXT
- HELP_DECRYPT.HTML
- HELP_DECRYPT.PNG
- HELP_DECRYPT.TXT
- HELP_DECRYPT.URL

A Figura 14mostra o arquivo Help_decrypt.txt aberto, com a sua nota e pedido de resgate.

Figura 14 – Arquivo Help_decrypt.txt aberto:

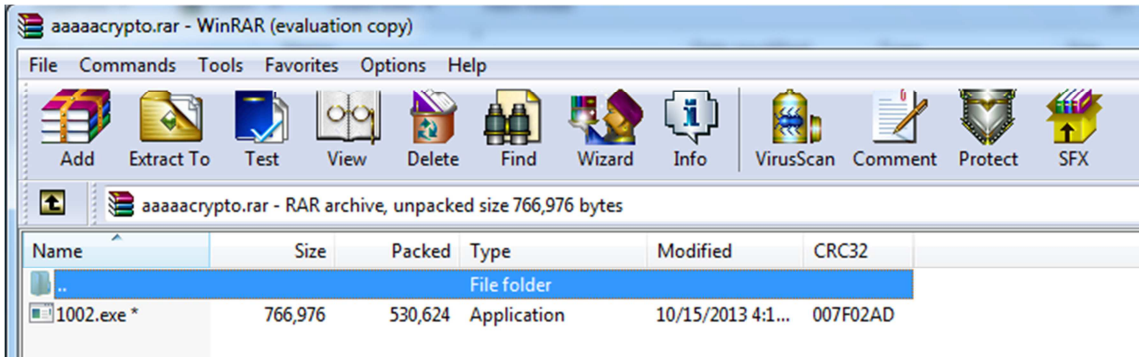


Fonte: Ransomware – Microsoft, Malware Protection Center1

6 Ambiente de teste

Preparou-se um ambiente de teste, através da criação de uma máquina virtual com Windows 7, onde possibilitou fazer algumas demonstrações, com a infecção de um vírus da família Ransomware, conhecido como CryptoLocker, que teve seu primeiro aparecimento em setembro de 2013. O vírus pode ser baixado em um repositório da máquina virtual, como um arquivo compactado. A Figura 15 ilustra o conteúdo do arquivo compactado, aberto com o software WinRAR.

Figura 15 – Winrar visualização do Vírus CryptoLocker :



Fonte: Autoria própria desenvolvida com ferramenta WinRAR.

Antes de executar o arquivo infectado, executamos um programa, chamado InstallWatch, uma ferramenta de comparação de sistema de arquivos baseado em Windows, capaz de comparar o conteúdo de seu sistema de arquivos e sistema de registros entre dois pontos no tempo. Após a execução do InstallWatch, executou-se o arquivo infectado qual foi realizado o download, a princípio não aconteceu nada visualmente.

Somente após a reinicialização da máquina virtual, e a obtenção de acesso a Internet é que o vírus veio se manifestar. Uma petição de resgate foi apresentada na área de trabalho, conforme ilustrado na Figura 16.

Figura 16 – Pedido de resgate:

Fonte: Autoria própria baseado em máquina virtual com Windows 7.

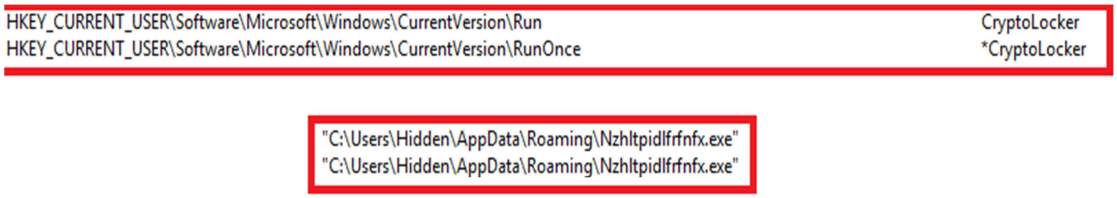
Novamente executou-se o programa InstallWatch, agora para fazer a comparação, do sistema de arquivos e registros antes da infecção do vírus e, após infecção pelo vírus. Observou-se a modificação de chaves *Run e RunOnce* no registro do Windows. As modificações destas chaves fazem com que programas sejam executados automaticamente cada vez que um usuário faz o *logon* na máquina.

Os programas executados nas chaves *RunOnce* são executados somente se o usuário tiver permissão para excluir entradas das respectivas chaves, além de serem executados sequencialmente. O Explorer aguarda até que cada um deles seja encerrado para continuar a execução normal. As chaves *RunOnce* se colocado o nome do valor com asterisco (*) força que o programa associado seja executado mesmo em modo de segurança.

As chaves *Run* são ignoradas quando o computador é iniciado no modo de segurança.

A Figura 17 mostra alteração que houve no registro do Windows, após a infecção do vírus de computador.

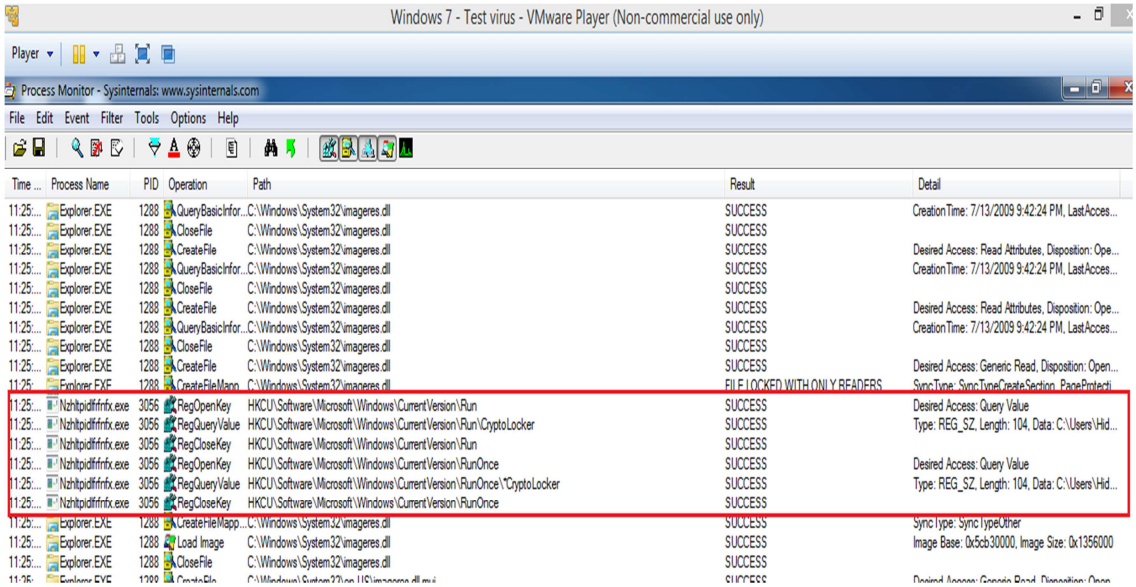
Figura 17 – Alteração registro do Windows



Fonte: Autoria própria desenvolvida com ferramenta InstallWatch.

Com o uso de outra ferramenta, chamada Process Monitor, uma ferramenta de monitoramento avançado do Windows que mostra atividade do sistema de arquivos em tempo real, registros, processos e thread. Observou-se também alterações de registro do Windows, da mesma forma que o programa InstallWatch, conforme pode ser observado na Figura 18.

Figura 18 – Alteração registro do Windows:



Fonte: Autoria própria desenvolvida com ferramenta Process Monitor.

6.1 Como prevenir-se

O Ransomware usa técnicas de infecção complexas e muito sofisticadas, o que faz com que a prevenção seja a melhor opção. Para isso é importante que se tenha um bom antivírus confiável instalado em seu computador e, que mantenha este atualizado. Tome precauções com os e-mails que contenha anexos, links para sites externos, se aparência de um e-mail é suspeito, cheio de erros ortográficos ou erros gramaticais ou se você não sabe quem é o remetente, deve-se ignorar este tipo de e-mail. Caso contrário, você poderá ser levado a clicar em um link mal intencionado ou fazer o download de um anexo infectado.

Tenha *backups* de todo o seu sistema de computador qual jugue ser importante para organização, guarde mais de uma cópia em mídias externas, como HD Externo, serviços em nuvem, como, Google Drive, pois o vírus ao infectar o computador, corrompe arquivos de *backups*, se estes estiverem na lista de extensões qual o vírus possa criptografar e acabar sequestrando o arquivo tomando posse deste.

Notou que a máquina foi infectada, desligue essa do acesso à Internet, pois como visto anteriormente, para iniciar o processo de encriptação dos arquivos o vírus precisa ter o acesso a Internet.

Conclusão

Neste trabalho abordámos o assunto de infecção de vírus de computador, do tipo Ransomware, que tem como propósito sequestrar os dados de sua vítima e criptografar os arquivos da máquina, como word, excel, pdf, etc. Verificou-se que para recuperar os arquivos novamente, os quais foram criptografados, teriam de pagar um valor de resgate ao criador do vírus, denominado Hacker. A principal forma de pagamento é através de moeda digital Bitcoin, em que pode-se manter em anonimato pois, há uma dificuldade de se rastrear este tipo de transação devido não ter um órgão regulamentador como governos, bancos envolvidos nessas transações. Porém pagar o resgate, não garante a solução do problema, pois não há garantia que conseguirá recuperar os arquivos infectados novamente.

Cumpriu-se alguns dos objetivos enunciados, pois como não se conseguiu obter uma versão atual do vírus da família Ransomware, alguns testes não puderam ser analisados por completo, como a verificação do vírus apagar os arquivos de sombra *Shadon Copy* do Windows, que serviriam como backup em uma eventualidade perdas de informação, como diz fazer a versão *Cryptowall 3.0* do vírus Ransomware.

O desenvolvimento do trabalho possibilitou compreender melhor como é o processo de infecção deste tipo de vírus, além de conceder que a prevenção ainda é a melhor solução, como ter backups em mais de um local, ter ferramentas para evitar a infecção deste tipo de vírus, como anti-malwares, antivírus atualizados, além de conscientizar os usuários à tomarem devidos cuidados com anexos de e-mail e atualizações falsas.

Referências

BERNSTEIN, Terry. **Segurança na internet**. Rio de Janeiro, Campus, 1997.

CISCO a, **Cryptowall 2.0**. Disponível em: <http://blogs.cisco.com/security/talos/cryptowall-2>. Acesso em 18 out. 2015.

CISCO b, **Cryptowall 3.0**. Disponível em: <http://blogs.cisco.com/security/talos/cryptowall-3-0>. Acesso em: 18 Out. 2015.

ENIGMAS SOFTWARE, **Cryptowall ransomware remoção**. Disponível em: <http://www.enigmasoftware.com/pt/cryptowallransomware-remocao/>. Acesso em 5 Set. 2015.

EXAME, **Ransomware:** Saiba tudo sobre os malwares sequestradores. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/ransomware-saiba-tudo-sobre-os-malware-sequestradores>. Acesso em 17 Out. 2015.

FEINSTEIN, Ken. **Faça de tudo para combater spam, vírus, pop-up & spyware**. Castelo Rio de Janeiro, Alta Books Ltda., 2005.

FONTES, Edison. **Segurança da Informação:** o usuário faz a diferença. São Paulo Saraiva, 2006.

GIZMODO BRASIL, **Tudo sobre bitcoin.** Disponível em: <http://gizmodo.uol.com.br/tudo-sobre-o-bitcoin/>. Acesso em 24 Out. 2015.

MALWARE PROTECTION CENTER, **Ransomware**. Disponível em: <https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx>. Acesso em 20 Out. 2015.

MALWARE PROTECTION CENTER, **Win32/Crowti**. Disponível em: <https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Win32%2fCrowti#tab=2>. Acesso em 22 Out. 2015.

PITKOWSKI, André. **Vírus:** prevenção, planejamento e controle, proteção de rede local, vírus mais comuns. São Paulo: Atlas S. A, 1992.

PKI – Public Key Infrastructure. <http://www.gta.ufrj.br/grad/07_2/delio/Criptografia.html>. Acessado em 5 Set. 2015.

SÊMOLA, Marcos. **Gestão da segurança da informação:** Uma visão executiva. 10. Reimpressão. Rio de Janeiro, RJ: Elsevier, 2003.

STALLING, William. **Criptografia e segurança de redes:** princípios e práticas. 4. Ed. São Paulo, Pearson Prentice Hall, 2007.